NEW ZEALAND

PATENT SPECIFICATION

270543

Priority Date(s): 10.3.94

Complete Specification Filed: 21.2.95

Classification (6): G06F15/16; G06F13/42; H04L12/22

Publication Date: 29 JAN 1997

P.O. Journal No: 1442

TRUE COPY

NEW ZEALAND

PATENTS ACT 1953

COMPLETE SPECIFICATION

" COMMUNICATION COMPUTER "

WE, ALCATEL AUSTRALIA LIMITED, (ACN 000 005 363)

A Company of the State of New South Wales, of 280 Botany Road, Alexandria, New South Wales, 2015, Australia, hereby declare the invention for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:

The invention relates to data transmission between networks and in particular to a communication computer for operation in a multi-computer system in which data is exchanged at several layers with the aid of defined protocols, said communication computer comprising an address bus and a data bus having at least one processor, at least one main memory, and control circuits for peripheral equipment connected thereto.

Data transmissions between locally separated data terminal equipment require declarations for protocols and messages, so that data exchange can take place in an intelligible form. In a local environment this can be achieved with locally observable rules . However, when data exchange is to occur between networks with different protocols, a corresponding matching of protocols becomes necessary which is usually conducted via gateways. To enable an unencumbered data exchange between modern communication systems which display a high degree of complexity and multiple functions, the different functions are schematically allocated to layers and suitable protocols defined for the various layers. The most common system of that kind is the OSI reference model (Open Systems Interconnection), a seven layer communication model determined by ISO (International Standard Organisation).

In principle, the communication systems can be linked at any one of the layers. Communication computers interact with each other and supply the required protocols. Usually the protocols are implemented by a

processor which is often responsible for other functions as well, for example processing another application. This however has some definite disadvantages, in particular when many communications coming from different layers are to be processed simultaneously. The gateway functions, i.e. the constantly necessary protocol conversions, pose a heavy workload for the processor at the expense of other processor functions. The individual protocols, although they are functionally and sequentially independent of each other are time coupled; furthermore, they are subject to a uniform operating system, although they make different requirements on an operating system.

With data transmission via networks which can be accessed by all kinds of users there is always the question of access control and data protection. Currently known solutions are based on functional expansions on one or more protocol layers, or define special intermediate protocol layers. Such measures do however suffer from several disadvantages. As there are no final standards for the discussed additions as yet, there is the danger of incompatibility due to the different implementations. A guaranteed safety cannot be achieved on this basis. And lastly, the additional safety functions increase the complexity of the protocols and require a larger processor performance.

Therefore, it is an object of the present invention to provide a communication computer in which bottlenecks created by processing

protocols are eliminated and which offers the highest possible data protection.

According to the invention, there is provided A communication computer for operation in a multi-computer system in which data is exchanged at several layers with the aid of defined protocols, said communication computer comprising an address bus and a data bus having at least one processor, at least one main memory, and control circuits for peripheral equipment connected thereto, wherein the communication computer further including a plurality of processors each of which is used for the handling of data at one protocol layer or at one permanently associated group of protocol layers.

The suggested communication computer is characterised in that it comprises a number of processors, each of which is used for the processing of data at associated protocol layers. A preferred form of embodiment provides a separate processor for each protocol layer. This arrangement permits time independent processing. based on matched operating systems for each processor. The mutual influencing of protocols is eliminated, delays remain small which results in a high data throughput.

A data processing system is known which comprises an encrypting/decrypting device between the central processing unit (CPU), ie. the processor and the data bus. This prevents unauthorised access to the processor. This principle can be applied to one or several processors of the

communication computer according to the present invention, so enabling the desired data protection.

In order that the invention may be readily carried into effect, an embodiment thereof will now be described in relation to the accompanying drawings, in which:

Figure 1 a schematic section of the communication computer according to the invention, and

Figure 2 the structure of the messages across the 7 OSI-layers with encryption on two layers.

Figure 1 shows the main part of the invention, a data processing system serving as communication computer. A total of eight processors is connected to a bus 8, as well as circuits such as main memory and peripheral controls which are not shown. Each of the processors is responsible for processing the messages of the associated layer of the OSI reference model, i.e. application processor 7 for layer 7, the Application Layer", presentation processor 6 for layer 6, the "Presentation Layer", session processor 5 for layer 5, the "Session Layer", transport processor 4 for layer 4 the "Transport Layer", the internetwork processor 3c and network processor 3a for layer 3, the "Network Layer", data protection processor 2 for layer 2, the "Datalink Layer"and bit transfer processor 1 for layer 1, the "Physical Layer". The use of two processors on the network level corresponds with the division of this layer into sub-layers 3ab for the

intranetwork communication, or 3c for the internetwork communication, which is used preferentially for network links via gateways.

It must be noted here, that the shown arrangement is preferred but not mandatory. It is also within the meaning of the invention to combine processors, in particular those whose protocols pose similar requirements to the operation of the processors, such as for example, the presentation processor 6 and the session processor 5. A completely independent processing is no longer possible to the full extent but it is possible that an overcapacity of processor performance can be avoided.

A special feature in the service of data protection is the encryption on individual layers, which is achieved, for example, with an encrypting and decrypting device 9, resp. 9' which is located between transport processor 4 and bus 8 or the data protection processor 2 and bus 8. The data and commands 10 transmitted between processor 4 and the encrypting/decrypting device 9 are not encrypted. The data and commands 11 which are sent to bus 8 from the encrypting/decrypting device 9 may be encrypted or not, depending upon requirement. The effect of encryption is described in more detail with the explanations for Figure 2. It must also be noted here, that the shown arrangement takes the character of an example. Encrypting can also be done in other ways. Encrypting/decrypting devices 9 can also be associated with other processors and in other numbers. The internetwork processor 3c is preferred because it processes the gateways to

third-party networks. The encrypting/decrypting device 9 is also able to transfer data directly without influencing it.

The physical structure of the multiprocessor computer can be implemented in many ways. This includes assemblies in their own, separate equipment, processor-bus linked processors in one unit and processors on a common board, with mixed versions also quite feasible.

Figure 2 shows the schematic arrangement of the messages, as they are structured and evaluated on the individual layers in accordance with the defaults of the OSI reference model. The eight processors are shown on the right-hand side, as they have been described in connection with Figure 1, however this time shown arranged on different levels above each other. Application processor 7 packs the data from an application into a processor suitable, standardised application message 17, which comprises two parts, the application informative-data, abbreviated to 7-data 27, and their socalled Header, the application-header data, abbreviated to 7-Header 37. This message is received as a whole on the underlying level 6 . The presentation processor 6 packs the data collecting on this level into a protocol -suitable, standardised presentation message 16, whose presentation informative-data, abbreviated to 6-data 26, contains the whole application message 17 of the overlying layer 7, and which also contains the presentation header-data, abbreviated to 6-Header 36. This process continues via the fifth level, the session layer with the session message 15, consisting of 5-data 25 and the

5-header 35, to the forth step, the transport layer.

Here then, in congruence with the assumption made for Figure 1, the first shading indicates the cryptography, the encryption of data and its decryption when the process is viewed from the reverse direction. Transport processor 4 is a cryptoprocessor as it is implemented, for example, by the arrangement according to Figure 1. Its output data, the transport message 14 is available in encrypted form. The used protocols and their function are not influenced by this. The data which is transferred to the underlying levels for further processing is now however encrypted and can only be decrypted by the receiving processor of the corresponding layer. An authorised participant in the communication system must therefore be a communication computer which comprises a cryptoprocessor on the same level and the corresponding key. In accordance with the agreement forming the basis of the layer model, header and data, i.e. the whole message of a layer, are always regarded as data by the lowerlying layer. The encryption carried out on the transport level in the example, is not recognisable on the lowerlying network level and neither is it on even lower levels. Only decrypted data is transferred to the session layer lying above.

In continuation of the described process, a partly encrypted intranetwork message 13a on the data protection level, on which according to assumption a cryptoprocessor acts, becomes part of the data protection message 12, which is encrypted as a whole. A part of the 2-data 22 is now

encrypted twice, while the 2-Header 32 and the remaining part of the 2-data 22 are encrypted once. The bit transfer processor 1 processes these data regardless into a bit transfer message 11 consisting of 1-Header 31 and 1-data 21. If the cryptoprocessor on the data protection level or its key is missing for one subscriber of the communication system, that subscriber cannot communicate at all. If the cryptoprocessor is missing on the transport level, it maintains connection but the transmitted information is not accessible for it.

Of course cryptography is possible on several or even all layers. Internetwork layer 3c which has been provided to link different networks in a network systems, is of particular importance. In this manner transitions between public, private and military networks are possible via corresponding gateways, thus necessitating a reliable control of access authorisation.

In principle, gateways are possible on all layers according to the OSI reference model. The use of specific processors for a particular layer enables processing the messages of this layer directly and so avoid protocol conversions. In a system of communication computers with processors for exclusively assigned protocol layers, the computers can communicate with each other via gateways on random protocol layers, without having to carry out computer internal protocol conversions dependent on the layer. This, together with cryptography, enables the aspect of data protection to be satisfactorily solved.

What we claim is:

1. A communication computer for operation in a multi-computer system in which data is exchanged at several layers with the aid of defined protocols, said communication computer comprising an address bus and a data bus having at least one processor, at least one main memory, and control circuits for peripheral equipment connected thereto, wherein the communication computer further including a plurality of processors each of which is used for the handling of data at one protocol layer or at one permanently associated group of protocol layers.

2. A communication computer as claimed in claim 1, including a plurality of processors each of which is used for the handling of data at precisely one permanently associated protocol layer.

3. A communication computer as claimed in claim 1 or claim 2, wherein the information transmitted between one to all selected processors and the data bus is encrypted.

4. A communication computer as claimed in claim 3, wherein the information transmitted between the processor responsible for Layer 3c of a ISO/OSI-7 reference model and the data bus is encrypted.

5. A communication computer as claimed in any one of the preceding claims, wherein it communicates via a gateway at an arbitrarily selectable layer having a processor of its own associated therewith, with the messages of a protocol layer being processed directly by the responsible processor,

270543

whereby the need for protocol conversions is eliminated.

6. A communication computer substantially as herein described with reference to Figures 1 - 2 of the accompanying drawings.

ALCATEL AUSTRALIA LIMITED

B. O'Connor

Authorized Agent P5/1/1703

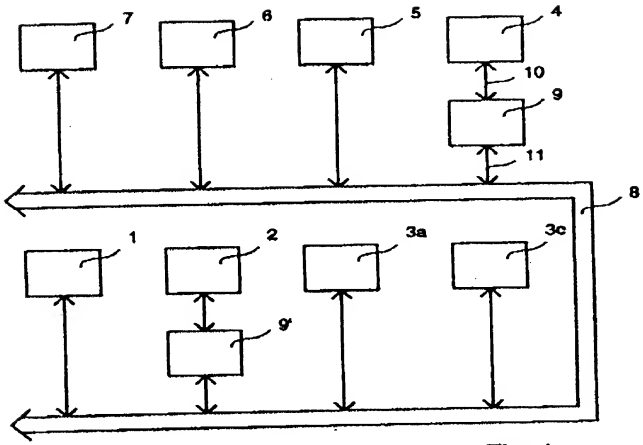

Fig. 1

ALCATEL AUSTRALIA LIMITED

B. O'Connor
Authorized Agent P5/1/1703

270543

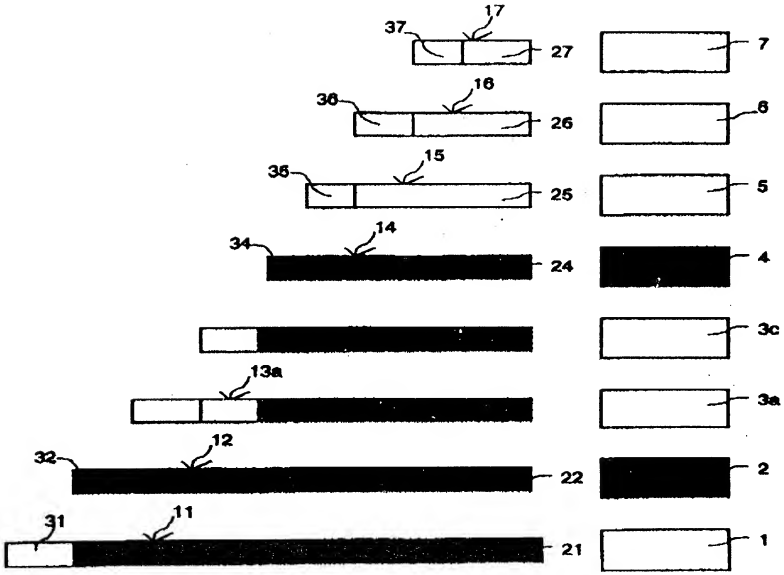

Fig. 2

ALCATEL AUSTRALIA LIMITED

B. O'Connor
Authorized Agent P5/1/1703